

# Release Notes

**FortiOS 7.0.3**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



January 10, 2022

FortiOS 7.0.3 Release Notes

01-703-765198-20220110

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction and supported models</b>	<b>6</b>
Supported models	6
<b>Special notices</b>	<b>7</b>
Azure-On-Demand image	7
GCP-On-Demand image	7
ALI-On-Demand image	7
Unsupported websites in SSL VPN web mode	8
RDP and VNC clipboard toolbox in SSL VPN web mode	8
FEC feature design change	8
<b>Upgrade information</b>	<b>9</b>
Fortinet Security Fabric upgrade	9
Downgrading to previous firmware versions	10
Firmware image checksums	11
IPsec interface MTU value	11
HA role wording changes	11
Strong cryptographic cipher requirements for FortiAP	11
How VoIP profile settings determine the firewall policy inspection mode	12
L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1	12
Add interface for NAT46 and NAT64 to simplify policy and routing configurations	12
Upgrading	12
Creating new policies	13
Example configurations	13
<b>Product integration and support</b>	<b>16</b>
Virtualization environments	16
Language support	17
SSL VPN support	18
SSL VPN web mode	18
<b>Resolved issues</b>	<b>19</b>
Security Fabric	19
Common Vulnerabilities and Exposures	19
<b>Known issues</b>	<b>20</b>
Anti Virus	20
Application Control	20
Endpoint Control	20
Explicit Proxy	21
Firewall	21
GUI	21
HA	22
IPsec VPN	23

---

Log & Report .....	23
Proxy .....	24
Security Fabric .....	24
SSL VPN .....	24
Switch Controller .....	24
System .....	25
User & Authentication .....	25
VM .....	26
WAN Optimization .....	26
WiFi Controller .....	26
<b>Limitations .....</b>	<b>28</b>
Citrix XenServer limitations .....	28
Open source XenServer limitations .....	28

# Change Log

Date	Change Description
2021-12-07	Initial release.
2021-12-13	Added <a href="#">RDP</a> and <a href="#">VNC</a> clipboard toolbox in <a href="#">SSL VPN web mode</a> on <a href="#">page 8</a> .
2021-12-28	Updated <a href="#">Resolved issues on page 19</a> and <a href="#">Known issues on page 20</a> .
2022-01-10	Updated <a href="#">Resolved issues on page 19</a> and <a href="#">Known issues on page 20</a> .

# Introduction and supported models

This guide provides release information for FortiOS 7.0.3 build 0237.

For FortiOS documentation, see the [Fortinet Document Library](#).

## Supported models

FortiOS 7.0.3 supports the following models.

<b>FortiGate</b>	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
<b>FortiWiFi</b>	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE
<b>FortiGate Rugged</b>	FGR-60F, FGR-60F-3G4G
<b>FortiGate VM</b>	FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
<b>Pay-as-you-go images</b>	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

# Special notices

- [Azure-On-Demand image on page 7](#)
- [GCP-On-Demand image on page 7](#)
- [ALI-On-Demand image on page 7](#)
- [Unsupported websites in SSL VPN web mode on page 8](#)
- [RDP and VNC clipboard toolbox in SSL VPN web mode on page 8](#)
- [FEC feature design change on page 8](#)

## Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

## GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

## ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

## Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1:

- Facebook
- Gmail
- Office 365
- YouTube

## RDP and VNC clipboard toolbox in SSL VPN web mode

Press **F8** to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1.

## FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
  edit <id>
    set fec enable
  next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.



# Upgrade information

Supported upgrade path information is available on the [Fortinet Customer Service & Support site](#).

## To view supported upgrade path information:

1. Go to <https://support.fortinet.com>.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
  - *Current Product*
  - *Current FortiOS Version*
  - *Upgrade To FortiOS Version*
5. Click *Go*.

## Fortinet Security Fabric upgrade

FortiOS 7.0.3 greatly increases the interoperability between other Fortinet products. This includes:

<b>FortiAnalyzer</b>	• 7.0.2
<b>FortiManager</b>	• 7.0.2
<b>FortiClient* Microsoft Windows</b>	• 7.0.0 build 0029 or later
<b>FortiClient* Mac OS X</b>	• 7.0.0 build 0022 or later
<b>FortiClient* Linux</b>	• 7.0.0 build 0018 or later
<b>FortiClient* iOS</b>	• 6.4.6 build 0507 or later
<b>FortiClient* Android</b>	• 6.4.6 build 0539 or later
<b>FortiClient* EMS</b>	• 7.0.0 build 0042 or later
<b>FortiAP FortiAP-S FortiAP-U FortiAP-W2</b>	• See <a href="#">Strong cryptographic cipher requirements for FortiAP on page 11</a>
<b>FortiSwitch OS (FortiLink support)</b>	• 6.4.6 build 0470 or later
<b>FortiSandbox</b>	• 2.3.3 and later, 4.0.0 is recommended

\* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC
14. FortiNAC
15. FortiVoice
16. FortiDeceptor
17. FortiAI
18. FortiTester



If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.3. When Security Fabric is enabled in FortiOS 7.0.3, all FortiGate devices must be running FortiOS 7.0.3.

---

## Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

## IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
  config ospf-interface
    edit "ipse-vpnx"
      set mtu-ignore enable
    next
  end
end
```

## HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

## Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1 and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE) will support strong ciphers in the future release of version 5.4.3.

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
  set tunnel-mode compatible
end
```

## How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

## L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1

**To make L2TP over IPsec work after upgrading:**

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2tp.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

## Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

## Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects > NAT46 Policy*
- *Policy & Objects > NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects > Virtual IPs* related pages

## Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip/vip6` and `ippool/ippool6`.

## Example configurations

`vip46` object:

Old configuration	New configuration
<pre>config firewall vip46   edit "test-vip46-1"     set extip 10.1.100.155     set mappedip 2000:172:16:200::55   next end</pre>	<pre>config firewall vip   edit "test-vip46-1"     set extip 10.1.100.150     set nat44 disable     <b>set nat46 enable</b>     set extintf "port24"     <b>set ipv6-mappedip</b>     <b>2000:172:16:200::55</b>   next end</pre>

`ippool6` object:

Old configuration	New configuration
<pre>config firewall ippool6     edit "test-ippool6-1"         set startip 2000:172:16:201::155         set endip 2000:172:16:201::155     next end</pre>	<pre>config firewall ippool6     edit "test-ippool6-1"         set startip 2000:172:16:201::155         set endip 2000:172:16:201::155         <b>set nat46 enable</b>     next end</pre>

NAT46 policy:

Old configuration	New configuration
<pre>config firewall policy46     edit 1         set srcintf "port24"         set dstintf "port17"         set srcaddr "all"         set dstaddr "test-vip46-1"         set action accept         set schedule "always"         set service "ALL"         set logtraffic enable         set ippool enable         set poolname "test-ippool6-1"     next end</pre>	<pre>config firewall policy     edit 2         set srcintf "port24"         set dstintf "port17"         set action accept         <b>set nat46 enable</b>         set srcaddr "all"         set dstaddr "test-vip46-1"         set srcaddr6 "all"         set dstaddr6 "all"         set schedule "always"         set service "ALL"         set logtraffic all         set ippool enable         set poolname6 "test-ippool6-1"     next end</pre>

vip64 object

Old configuration	New configuration
<pre>config firewall vip64     edit "test-vip64-1"         set extip 2000:10:1:100::155         set mappedip 172.16.200.155     next end</pre>	<pre>config firewall vip6     edit "test-vip64-1"         set extip 2000:10:1:100::155         set nat66 disable         <b>set nat64 enable</b>         <b>set ipv4-mappedip 172.16.200.155</b>     next end</pre>

ippool object

Old configuration	New configuration
<pre>config firewall ippool     edit "test-ippool4-1"</pre>	<pre>config firewall ippool     edit "test-ippool4-1"</pre>

Old configuration	New configuration
<pre>set startip 172.16.201.155 set endip 172.16.201.155 next end</pre>	<pre>set startip 172.16.201.155 set endip 172.16.201.155 <b>set nat64 enable</b> next end</pre>

NAT64 policy:

Old configuration	New configuration
<pre>config firewall policy64 edit 1 set srcintf "wan2" set dstintf "wan1" set srcaddr "all" set dstaddr "test-vip64-1" set action accept set schedule "always" set service "ALL" set ippool enable set poolname "test-ippool4-1" next end</pre>	<pre>config firewall policy edit 1 set srcintf "port24" set dstintf "port17" set action accept <b>set nat64 enable</b> set srcaddr "all" set dstaddr "all" set srcaddr6 "all" set dstaddr6 "test-vip64-1" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname "test-ippool4-1" next end</pre>

# Product integration and support

The following table lists FortiOS 7.0.3 product integration and support information:

<b>Web browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Edge 94</li><li>• Mozilla Firefox version 93</li><li>• Google Chrome version 94</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.
<b>Explicit web proxy browser</b>	<ul style="list-style-type: none"><li>• Microsoft Edge 44</li><li>• Mozilla Firefox version 74</li><li>• Google Chrome version 80</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.
<b>FortiController</b>	<ul style="list-style-type: none"><li>• 5.2.5 and later</li></ul> Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
<b>Fortinet Single Sign-On (FSSO)</b>	<ul style="list-style-type: none"><li>• 5.0 build 0302 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none"><li>• Windows Server 2019 Standard</li><li>• Windows Server 2019 Datacenter</li><li>• Windows Server 2019 Core</li><li>• Windows Server 2016 Datacenter</li><li>• Windows Server 2016 Standard</li><li>• Windows Server 2016 Core</li><li>• Windows Server 2012 Standard</li><li>• Windows Server 2012 R2 Standard</li><li>• Windows Server 2012 Core</li><li>• Windows Server 2008 64-bit (requires Microsoft SHA2 support package)</li><li>• Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)</li><li>• Windows Server 2008 Core (requires Microsoft SHA2 support package)</li><li>• Novell eDirectory 8.8</li></ul></li></ul>
<b>FortiExtender</b>	<ul style="list-style-type: none"><li>• 4.0.0 and later, 7.0.3 is recommended</li></ul>
<b>AV Engine</b>	<ul style="list-style-type: none"><li>• 6.00266</li></ul>
<b>IPS Engine</b>	<ul style="list-style-type: none"><li>• 7.00043</li></ul>

## Virtualization environments

The following table lists hypervisors and recommended versions.



Hypervisor	Recommended versions
<b>Citrix Hypervisor</b>	<ul style="list-style-type: none"> <li>8.1 Express Edition, Dec 17, 2019</li> </ul>
<b>Linux KVM</b>	<ul style="list-style-type: none"> <li>Ubuntu 18.0.4 LTS</li> <li>Red Hat Enterprise Linux release 8.4</li> <li>SUSE Linux Enterprise Server 12 SP3 release 12.3</li> </ul>
<b>Microsoft Windows Server</b>	<ul style="list-style-type: none"> <li>2012R2 with Hyper-V role</li> </ul>
<b>Windows Hyper-V Server</b>	<ul style="list-style-type: none"> <li>2019</li> </ul>
<b>Open source XenServer</b>	<ul style="list-style-type: none"> <li>Version 3.4.3</li> <li>Version 4.1 and later</li> </ul>
<b>VMware ESX</b>	<ul style="list-style-type: none"> <li>Versions 4.0 and 4.1</li> </ul>
<b>VMware ESXi</b>	<ul style="list-style-type: none"> <li>Versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.</li> </ul>

## Language support

The following table lists language support information.

### Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

## SSL VPN support

### SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

#### Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 89 Google Chrome version 91
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 94 Google Chrome version 96
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 94 Google Chrome version 96
macOS Big Sur 11.2	Apple Safari version 14 Mozilla Firefox version 92 Google Chrome version 93
macOS Monterey 12.0	Apple Safari version 15 Mozilla Firefox version 94 Google Chrome version 96
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

## Resolved issues

The following issues have been fixed in version 7.0.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Security Fabric

Bug ID	Description
753358	Unable to trigger automation trigger with FortiDeceptor Fabric event.

## Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE references
752134	FortiOS 7.0.3 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2021-42757</li></ul>

# Known issues

The following issues have been identified in version 7.0.3. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Anti Virus

Bug ID	Description
723686	The partial fetch handling in the IMAP proxy only detects and scans the first fetched section, which allows threats in subsequent fetched sections to go through the firewall undetected.

## Application Control

Bug ID	Description
752569	Per IP shaper under application list does not work as expected for some applications.

## Endpoint Control

Bug ID	Description
708545	The WAD daemon is triggered to fetch the FortiClient information based on a ZTNA EMS tag enabled for checking in a proxy policy. It is then possible to get a ZTNA EMS tag in the firewall dynamic address and get the expected traffic control.
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. <b>Workaround:</b> delete the EMS Cloud entry then add it back.
744613	EMS endpoint IP and MAC addresses are not synchronized to the ZTNA tags on the FortiGate.

## Explicit Proxy

Bug ID	Description
664380	When configuring explicit proxy with forward server, if <code>ssl-ssh-profile</code> is enabled in <code>proxy-policy</code> , WAD is unable to correctly learn the destination type correctly, so the destination port is set to 0, but the squid proxy server does not accept the request and returns an error.

## Firewall

Bug ID	Description
739949	In HA vcluster scenario, the <i>Bytes</i> counter on the <i>Firewall Policy</i> page always shows <i>0 B</i> for the secondary while the <i>Edit Policy</i> page shows the correct <i>Total bytes</i> in the statistics.
746891	Auto-update script sent from FortiOS GUI has a policy ID of zero, which causes FortiManager to be out of synchronization.

## GUI

Bug ID	Description
440197	On the <i>System &gt; FortiGuard</i> page, the override FortiGuard server for <i>AntiVirus &amp; IPS Updates</i> shows an <i>Unknown</i> status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
663558	When logging in to a VDOM in the GUI with JSConsole, the system event log displays an incorrect IP address.
685431	On the <i>Policy &amp; Objects &gt; Firewall Policy</i> page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. <b>Workaround:</b> use the CLI to configure policies.
707589	<i>System &gt; Certificates</i> list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. <b>Workaround:</b> use Chrome, Edge, or Safari as the browser.
713529	When FortiAnalyzer is configured, the HTTPS daemon may crash while processing some FortiAnalyzer log requests. There is no apparent impact on the GUI operation.

Bug ID	Description
714455	CLI shows EMS tag object in the address select list, but it is not available in the GUI omni select list.
729324	<i>Managed FortiAPs</i> and <i>Managed FortiSwitches</i> pages keep loading when VDOM administrator has <code>netgrp</code> and <code>wifi</code> read/write permissions.
730466	The search does not work on the <i>Policy &amp; Objects &gt; Addresses</i> page if there is a non-EMS address group with an EMS tag (invalid configuration).
730533	Improve GUI error message for SSL VPN policy with VIPs or virtual servers that have web mode is enabled.
735248	On a mobile phone, the WiFi captive portal may take longer to load when the default firewall authentication login template is used and the user authentication type is set to HTTP. <b>Workaround:</b> edit the login template to disable HTTP authentication or remove the href link to googleapis.
738027	The <i>Device Inventory</i> widget shows <i>no results</i> when there are two <code>user_info</code> parameters. <b>Workaround:</b> use the CLI to retrieve the device list.
742626	The VDOM dropdown list in the banner should be scrollable.
746953	On the <i>Network &gt; Interfaces</i> page, users cannot modify the TFTP server setting. A warning with the message <i>This option may not function correctly. It is already configured using the CLI attribute: tftp-server.</i> appears beside the <i>DHCP Options</i> entry. <b>Workaround:</b> use the CLI.
748010	When creating or editing a ZTNA rule from the GUI, users cannot select the <i>any</i> option interface for <i>Incoming Interface</i> . Users can still configure this option in the CLI.
748530	A gateway of <code>0.0.0.0</code> is not accepted in a policy route.
749451	On the <i>Network &gt; SD-WAN</i> page, the volume sent/received displayed in the charts does not match the values provided from the REST API when the RX and TX values of <code>diagnose sys sdwan intf-sla-log</code> exceed $2^{32}-1$ .
750490	Firewall policy changes made in the GUI remove the replacement message group in that policy.
755177	When upgrade firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
756420	The connection to FortiManager is shown as down when there is a connection.
757130	After upgrading, the new ACME certificates configured in the GUI are using the staging environment.

## HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.

Bug ID	Description
701367	In an HA environment with multiple virtual clusters, <i>System &gt; HA</i> will display statistics for <i>Uptime</i> , <i>Sessions</i> , and <i>Throughput</i> under virtual cluster 1. These statistics are for the entire device. Statistics are not displayed for any other virtual clusters.
729719	When enabling <code>ha-direct</code> , some invalid configurations should be reset and hidden.
730770	After a hasync crash, the FGFM process stops sending keepalives.
732201	VDOM restore on an already configured VDOM causes high CPU sometimes on the primary.
738934	No GARP is being sent out on the VWP interface upon HA failover, causing a long failover time.
740933	HA goes out of synchronization when uploading a local certificate.
750004	The secondary FortiGate shows a DHCP IP was removed due to conflict, but it is not removed on the primary FortiGate.

## IPsec VPN

Bug ID	Description
715671	Traffic is failing on dialup VPN IKEv2 with EAP authentication.
740475	Traffic cannot be sent out through IPsec VPN tunnel because SA is pushed to the wrong NP6 for platforms where NP6 is standalone. Affected models: FG-2000E and FG-2500E.
740624	<p>FortiOS 7.0 has new design for dialup VPN (no more route tree in the IPsec tunnel), so traffic might not traverse over the dialup IPsec VPN after upgrading from FortiOS 6.4.6 to 7.0.1, 7.0.2, or 7.0.3 if the server replies on the static route over the dynamic tunnel interface to route the traffic back to the client.</p> <p><b>Workaround:</b> configure the <code>src-subnet</code> on the client phase 2 interface. Then, static routes will be added by IKE on the server side (<code>add-route enable</code> is required).</p> <pre>config vpn ipsec phase2-interface     edit &lt;name&gt;         set src-subnet &lt;x.x.x.x/x&gt;     next end</pre>

## Log & Report

Bug ID	Description
747854	PDF report generation fails due to an HPDF API error when it is drawing a circle and there is only one entry in the SQL result.

## Proxy

Bug ID	Description
712584	WAD memory leak causes device to go into conserve mode.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.
758122	WAD memory usage may spike and cause the FortiGate to enter conserve mode when downloading a large file fails.

## Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
748389	Security Fabric automation email action trigger shows multiple emails as one email with no separation between the addresses.
753056	Recommendation information for <i>Failed Login Attempts</i> security rating rule should display <i>Lockout duration should be at least 30 minutes</i> , instead of 1800 minutes.
755187	The security rating test for <i>Unused Policies</i> is incorrectly evaluated as <i>Pass</i> when there are unused policies with the accept action.

## SSL VPN

Bug ID	Description
737894	If there are no users or groups in an SSL VPN policy, the SSL VPN daemon may crash when an FQDN is a destination address in the firewall policy.
753515	DTLS does not work for SSL VPN and switches to TLS.

## Switch Controller

Bug ID	Description
740661	FortiGate loses FortiSwitch management access due to excessive configuration pushes.



## System

Bug ID	Description
572847	The wan1, wan2, and dmz interfaces should not be configured as hardware switch members on the 60F series. The wan interface should not be configured as a hardware switch member on the 40F series.
596942	SoC3 platforms may encounter kernel panic in cases when a PKCE IOCTL wait event is interrupted by WAD diagnose CLI commands.
639861	Support FEC (forward error correction) implementations in 10G, 25G, 40G, and 100G interfaces for FG-3400E and FG-3600E.
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
675558	SFP port with 1G copper SFP always is up.
679035	NP6 drops, and bandwidth is limited to under 10 Gbps in <code>npu-vlink</code> case.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
683299	Port group members have different speeds after the port speed is changed using a CLI script.
685674	FortiGate did not restart after restoring backup configuration.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
716341	SFP28 port flapping when the speed is set to 10G.
741359	As per IEEE 802.3, NP frames under 64 octets should be discarded on the RX.
755953	Direct CLI script from FortiManager fails due to additional <code>end</code> at the end of <code>diagnose debug crashlog read</code> .
756713	Packet Loss on the LAG interface (eight ports) in static mode. Affected models: FG-110xE, FG-220xE, and FG-330xE.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.

## User & Authentication

Bug ID	Description
750551	DST_Root_CA_X3 certificate is expired. <b>Workaround:</b> see the Fortinet PSIRT blog, <a href="https://www.fortinet.com/blog/psirt-blogs/fortinet-and-expiring-lets-encrypt-certificates">https://www.fortinet.com/blog/psirt-blogs/fortinet-and-expiring-lets-encrypt-certificates</a> , for more information.
756763	In the email collection captive portal, a user can click <i>Continue</i> without selecting the checkbox to accept the terms and disclaimer agreement.

Bug ID	Description
757883	FortiGate blocks expired root CA, even if the cross-signed intermediate CA of the root CA is valid.
765136	Dynamic objects are cleared when there is no connection between the FortiGate and FortiManager with NSX-T.

## VM

Bug ID	Description
689047	ARM64-KVM has kernel panic.
691337	When upgrading from 6.4.7 to 7.0.2, GCP SDN connector entries that have a <code>gcp-project-list</code> configuration will be lost.

## WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when <code>wanopt</code> is set to manual mode and an external proxy is used. <b>Workaround:</b> set <code>wanopt</code> to automatic mode, or set <code>transparent disable</code> in the <code>wanopt</code> profile.
754378	When an AV profile is enabled in a WANOpt proxy policy on a server side FortiGate, EICAR sent over HTTPS will not get blocked.

## WiFi Controller

Bug ID	Description
578440	Wireless controller sends ARP request packets that are destined to the FortiGate back to all tunnel interfaces.
600257	FG-1000D and FG-1500D go in to conserve mode when <code>wpad</code> and <code>cw_acd</code> have a memory spike, which affects wireless user tunnel traffic.
675164	FWF-60F local radio shows WPA3 is not supported.
726266	GUI becomes unresponsive on FWF-60E with a wrong WTP entry.
727301	Unable to quarantine hosts behind FortiAP and FortiSwitch.

Bug ID	Description
744687	Client should match the new NAC policy if it is reordered to the top one.
745044	Optimize memory usage of wpad daemon in WiFi controller for large-scale 802.11r fast BSS transition deployment.
748479	cw_acd is crashing with signal 11 and is causing APs to disconnect/rejoin.
751509	On FAP-U432F, the <i>Radio 3</i> spectrum analysis should be disabled in the FortiGate GUI.

# Limitations

## Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

## Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.